




Ejercicio Práctico

 **Título:** Análisis de Reconocimiento Activo y Detección de Vulnerabilidades con Nmap y OpenVAS

Objetivo del ejercicio:

Aplicar técnicas avanzadas de **reconocimiento activo** y **escaneo de vulnerabilidades**, utilizando **Nmap** y **OpenVAS**, para identificar servicios expuestos, versiones vulnerables y realizar una evaluación técnica de seguridad sobre un objetivo en un entorno controlado.

Escenario:

Eres parte de un equipo de pruebas de penetración en un laboratorio de ciberseguridad. Se te ha asignado la IP de una máquina objetivo vulnerable (**192.168.56.110**). Tu misión es identificar la infraestructura técnica expuesta utilizando comandos de reconocimiento activo y herramientas de escaneo, y analizar posibles vulnerabilidades para redactar un informe técnico básico.

Tu tarea:

Paso 1 – Reconocimiento activo del objetivo

1. Usa comandos como **nslookup** y **dig** para obtener información sobre el dominio o IP asignada:

```
nslookup 192.168.56.110
dig -x 192.168.56.110
```

2. Registra la información obtenida: nombre del host, registros DNS, y cualquier dato útil.

✓ Paso 2 – Escaneo de puertos y servicios

1. Ejecuta los siguientes comandos desde Kali Linux:

```
nmap -sS -sV -O 192.168.56.110  
nmap --script=vuln 192.168.56.110
```

2. Registra los siguientes datos:
 - Puertos abiertos
 - Servicios detectados
 - Versiones de software
 - Resultados de scripts NSE (vulnerabilidades)

✓ Paso 3 – Análisis con OpenVAS

1. Accede a la interfaz web de OpenVAS desde Kali:

<https://localhost:9392/>

2. Crea una nueva tarea:
 - Objetivo: 192.168.56.110
 - Escaneo completo y profundo
3. Espera los resultados y descarga el reporte.

✓ Paso 4 – Interpretación del informe

1. Revisa las vulnerabilidades críticas (CVSS alto) encontradas.

2. Selecciona al menos una e investiga:

- Nombre y descripción
 - CVE asociado
 - Riesgo e impacto potencial
 - Cómo se puede explotar
-

Paso 5 – Recomendaciones técnicas

1. Propón **tres acciones correctivas** para mitigar los riesgos detectados.
 2. Redacta un breve párrafo explicando por qué el escaneo debe hacerse de forma ética y bajo autorización formal.
-

Resultado esperado:

- Reporte de escaneo Nmap detallado
 - Informe generado por OpenVAS
 - Identificación y documentación de una vulnerabilidad crítica
 - Propuesta de mitigación técnica
 - Reflexión ética argumentada
-

Reflexión Final:

¿Qué aprendiste al usar herramientas como Nmap y OpenVAS?
¿Cómo contribuye el análisis activo a una auditoría completa?
¿Qué precauciones se deben tomar al realizar estos ejercicios en ambientes reales?
